UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/010,959	11/30/2001	Mark Muhlestein	67272-8128.US02	5673

77042 7590 02/03/2009

Perkins Coie LLP
P.O. Box 1208
Seattle, WA 98111-1208

EXAMINER	
KHOSHNOODI, NADIA	
ART UNIT	PAPER NUMBER
2437	
MAIL DATE	DELIVERY MODE
02/03/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/010,959	MUHLESTEIN, MARK	
	Examiner	Art Unit	
	NADIA KHOSHNOODI	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11/12/2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *76-95* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *76-95* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 November 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

Claims 1-75 are cancelled. Applicant's arguments/amendments with respect to previously presented claims 76-90 and newly presented claims 91-95 filed 11/12/2008 have been fully considered and therefore the claims are rejected under new grounds. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

Response to Arguments

Applicants have requested that the Examiner "cite a prior art reference to support the taking of official notice, as required by MPEP 2144.03(c)." Examiner would like to point out that in the previous office action mailed 7/3/2008, the section appearing before the conclusion labeled "References Cited, Not Used" listed several references to support the portions that Examiner took official notice on. Specifically, Examiner would like to direct Applicants attention to ***US Patent No. 6,108,785; US Patent No. 5,396,609; and US Pub. No. 2004/0226010*** for supporting evidence that the limitations "assigning a specific access type to the processing device by the storage server when the storage server verifies the processing device satisfies restriction criteria," was commonly known in the art at the time this invention was made.

Allowable Subject Matter

Claims 80-81, 84-85, 87, 89, and 91 are objected to as being dependent upon a rejected base claim (due to the Double Patenting Rejection necessitated by the amendments set forth

below), but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Double Patenting

I. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

II. Claims 76-85 and 93 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1 of US Patent No. 7,346,928 in view of EP 0903 901 A2 and US Pub. No. 2004/0226010.

Although the conflicting claims are not identical, they are not patentably distinct from each other because independent claim 1 from US Patent No. 7,346,928 substantially teaches steps for carrying out the following limitations: receiving at the storage server, requests for files maintained at the storage server from at least one client; causing by the storage server, each of a

plurality of cluster devices external to the storage server to execute an operation on the files; at the storage server receiving results of the plurality of cluster devices' operations on the files; conveying an outcome of the results to at least one of the clients, where the operation is a virus scan and the file path of the files is taken into consideration in order to execute an operation.

Not explicitly disclosed is selecting, at the storage server, the processing device from among a plurality of processing devices that form the cluster, based on a classification of the processing device relative to the other processing devices in the cluster, wherein the classification is based on a performance criterion. However, Takahashi et al. teach that the request is assigned to a clustered device that has the smallest load on it at the time the request is received (par. 24). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in US Patent No. 7,346,928 to classify the processing devices based on performance criterion. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Takahashi et al. suggest that distributing packages to various processing devices based on the load and how quickly the device is able to handle requests results in faster processing time in par. 85-88.

Also not explicitly disclosed is assigning a specific access type to the processing device by the storage server when the storage server verifies the processing device satisfies restriction criteria. However, Suorsa teaches assigning different levels of trust to different devices (par. 50). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in US Patent No. 7,346,928 to assign a specific access type to a processing device by the storage server to verify that the processing device satisfies restriction

criteria. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Suorsa suggests that various processing devices may be assigned a lower level of trust in order to prevent them from accessing unauthorized information on the storage server in par. 50.

II. Claims 86-92 and 94-95 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1 of US Patent No. 7,346,928 in view of EP 0903 901 A2; US Pub. No. 2004/0226010; and US Patent No. 4,104,718.

Although the conflicting claims are not identical, they are not patentably distinct from each other because independent claim 1 from US Patent No. 7,346,928 substantially teaches steps for carrying out the following limitations: receiving at the storage server, requests for files maintained at the storage server from at least one client; causing by the storage server, each of a plurality of cluster devices external to the storage server to execute an operation on the files; at the storage server receiving results of the plurality of cluster devices' operations on the files; conveying an outcome of the results to at least one of the clients, where the operation is a virus scan and the file path of the files is taken into consideration in order to execute an operation.

Not explicitly disclosed is selecting, at the storage server, the processing device from among a plurality of processing devices that form the cluster, based on a classification of the processing device relative to the other processing devices in the cluster, wherein the classification is based on a performance criterion. However, Takahashi et al. teach that the request is assigned to a clustered device that has the smallest load on it at the time the request is received (par. 24). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in US Patent No. 7,346,928 to classify the

processing devices based on performance criterion. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Takahashi et al. suggest that distributing packages to various processing devices based on the load and how quickly the device is able to handle requests results in faster processing time in par. 85-88.

Also not explicitly disclosed is assigning a specific access type to the processing device by the storage server when the storage server verifies the processing device satisfies restriction criteria. However, Suorsa teaches assigning different levels of trust to different devices (par. 50). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in US Patent No. 7,346,928 to assign a specific access type to a processing device by the storage server to verify that the processing device satisfies restriction criteria. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Suorsa suggests that various processing devices may be assigned a lower level of trust in order to prevent them from accessing unauthorized information on the storage server in par. 50.

Finally not explicitly disclosed is wherein the specific access type allows the processing device to perform the operation even while another user has a lock on the object. However, Poublan et al. teach that it is well known that, depending on the particular lock the user has put on the file, reading of the file is still permitted by other processes (where virus-scanning is a "read"-type operation as opposed to a "write" operation). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in US Patent No. 7,346,928 to allow for the processing device to perform an operation, such as virus

scanning on the object even while another user has a lock on the object. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Poublan et al. suggest that if a "for input" lock is the type of lock placed on a file by a user, other processes may still access the file for reading purposes, where this is beneficial so that authorized users may access resources as needed for their duties in col. 63, lines 57-63.

Claim Rejections - 35 USC § 103

III. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

IV. Claims 76-77, 79, 82-83, and 93 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bates et al., US Patent No. 6,721,721, and further in view of Edwards et al., US Patent No. 6,931,540 and that which is commonly known in the art.

As per claims 76 and 82:

Bates et al. substantially teach a method/apparatus including: receiving at a storage server, from a requester, a request for an object stored at the server (col. 4, lines 35-44); in response to the request, determining whether to cause a processing device in a cluster of processing devices access to the object, wherein the cluster is separate from the storage server and is not in a path from the requester to the object (col. 6, lines 25-34); causing the processing device to perform the operation in response to a specified outcome of said determining (col. 7,

line 60 – col. 8, line 3); receiving at the storage server a result of the operation from the processing device (col. 8, lines 23-30 and col. 8, lines 44-48); and conditionally allowing access to the object in response to the request according to the result of the operation (col. 9, lines 10-20 and col. 11, lines 55-67).

Not explicitly disclosed is wherein the determining step includes determining at the storage server whether to cause a processing device to access the object stored at the storage server and perform an operation on data associated with the object based at least partially on a file space containing the object. However, Edwards et al. teach that various processing devices perform various scan types depending on the type of file which is requested to be scanned (col. 5, lines 1-12 and lines 35-39). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Bates et al. to determine whether a processing device has proper access to perform a particular virus scan on the file at hand. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Edwards et al. suggest that varying levels of security are utilized depending on the process accessing the file, as well as the type of file being accessed in order to allow for better/more efficient use of the systems resources in col. 3, line 60 – col. 4, line 10.

Also not explicitly disclosed is assigning a specific access type to the processing device by the storage server when the storage server verifies the processing device satisfies restriction criteria. The Examiner takes official notice that it is commonly known and widely practiced for the scanning process to be on a device that is assigned a particular access type based on its location in the network, i.e. devices more susceptible to attacks may be given less access than

those which are not as vulnerable. It would be obvious to a person skilled in the art to associate the device with a particular access type in order to prevent from various devices gaining unauthorized access to various facilities.

Finally not explicitly disclosed is selecting, at the storage server, the processing device from among a plurality of processing devices that form the cluster, based on classification of the processing device relative to other processing devices in the cluster, wherein the classification is based on performance criteria. However, Bates et al. also suggest distributing the load of generating virus status information (col. 7, line 57- col. 8, line 3). The Examiner takes official notice that it is commonly known and widely practiced in clustered environments to delegate requests to clusters based on their particular load at the time. It would be obvious to a person skilled in the art to assign a particular device within a cluster to a request based on the load on that the device is experiencing at the time the request is received in order to process requests faster within the cluster.

As per claims 77 and 90:

Bates et al. and Edwards et al. substantially teach the method/apparatus of claims 76 and 82. Furthermore, Edwards et al. teach wherein the operation includes a plurality of processes (col. 3, lines 60-66). Bates et al. further teach each process being performed at a separate processing device in the cluster (col. 4, lines 48-55).

As per claims 79 and 83:

Bates et al. and Edwards et al. substantially teach the method/apparatus of claims 76 and 82. Furthermore, Bates et al. teach wherein the storage server enforces a timeout for the operation; wherein even if the timeout expires, the processing device completes the operation

and reports the result of the operation to the server; and wherein the storage server stores the result of the operation for possible later use (col. 8, lines 16-48).

V. Claims 78 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bates et al., US Patent No. 6,721,721, Edwards et al., US Patent No. 6,931,540, and that which is commonly known in the art, as applied to claim 76 above, and further in view of Poublan et al., US Patent No. 4,104,718.

As per claim 78:

Bates et al. and Edwards et al. substantially teach the method of claim 76. Furthermore, Edwards et al. teach the method further including assigning a specific access type to the processing device by the server, the specific access type allowing the processing device to perform the operation (col. 3, lines 45-59). Not explicitly disclosed is wherein the specific access type allows the processing device to perform the operation even while another user has a lock on the object. However, Poublan et al. teach that it is well known that, depending on the particular lock the user has put on the file, reading of the file is still permitted by other processes (where virus-scanning is a "read"-type operation as opposed to a "write" operation). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Bates et al. and Edwards et al. to allow for the processing device to perform an operation, such as virus scanning on the object even while another user has a lock on the object. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Poublan et al. suggest that if a "for input" lock is the type of lock placed on a file by a user, other processes

may still access the file for reading purposes, where this is beneficial so that authorized users may access resources as needed for their duties in col. 63, lines 57-63.

VI. Claims 86, 88, 90, 92, and 94-95 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bates et al., US Patent No. 6,721,721 and further in view of Poublan et al., US Patent No. 4,104,718 and that which is commonly known in the art.

As per claims 86 and 90:

Bates et al. substantially teach a method/system including: receiving at a storage server a client request for an object stored at the server (col. 4, lines 35-44); the processing device separate from the storage server and is not in a path from the client to the object (col. 6, lines 25-34); causing the processing device to perform the operation (col. 7, line 60 – col. 8, line 3); receiving at the storage server a result of the operation from the processing device (col. 8, lines 23-30 and lines 44-48); and conditionally allowing access to the object in response to the client request according to the result of the operation (col. 9, lines 10-20 and col. 11, lines 55-67).

Not explicitly disclosed is that the specific access type allows the processing device to perform an operation on the object even while another client has a lock on the object. However, Poublan et al. teach that it is well known that, depending on the particular lock the user has put on the file, reading of the file is still permitted by other processes (where virus-scanning is a "read"-type operation as opposed to a "write" operation). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method/system disclosed in Bates et al. and Edwards et al. to allow for the processing device to perform an operation, such as virus scanning on the object even while another user has a lock on the object. This modification would have been obvious because a person having ordinary skill in the art, at the

time the invention was made, would have been motivated to do so since Poublan et al. suggest that if a "for input" lock is the type of lock placed on a file by a user, other processes may still access the file for reading purposes, where this is beneficial so that authorized users may access resources as needed for their duties in col. 63, lines 57-63.

Also not explicitly disclosed is assigning a specific access type to the processing device by the storage server when the storage server verifies the processing device satisfies restriction criteria. The Examiner takes official notice that it is commonly known and widely practiced for the scanning process to be on a device that is assigned a particular access type based on its location in the network, i.e. devices more susceptible to attacks may be given less access than those which are not as vulnerable. It would be obvious to a person skilled in the art to associate the device with a particular access type in order to prevent from various devices gaining unauthorized access to various facilities.

Finally not explicitly disclosed is selecting, at the storage server, the processing device from among a plurality of processing devices that form the cluster, based on classification of the processing device relative to other processing devices in the cluster, wherein the classification is based on performance criteria. However, Bates et al. also suggest distributing the load of generating virus status information (col. 7, line 57- col. 8, line 3). The Examiner takes official notice that it is commonly known and widely practiced in clustered environments to delegate requests to clusters based on their particular load at the time. It would be obvious to a person skilled in the art to assign a particular device within a cluster to a request based on the load on that the device is experiencing at the time the request is received in order to process requests faster within the cluster.

As per claim 88:

Bates et al. substantially teach an apparatus comprising: a storage server storing a set of objects and having a network interface (col. 4, lines 35-44); and a processing device coupled to the server, wherein the processing device is one of a plurality of processing devices configured as a cluster which is not in a path from a client to the objects stored at the server (col. 6, lines 25-34), wherein: the storage server receives a client request for an object of the set of objects through the network interface (col. 4, lines 35-44); the storage server causes the processing device to perform the operation (col. 7, line 60 – col. 8, line 3); the storage server receives at the storage server a result of the operation from the processing device (col. 8, lines 23-30 and lines 44-48); and the storage server conditionally allows access to the object in response to the client request according to the result of the operation (col. 9, lines 10-20 and col. 11, lines 55-67).

Not explicitly disclosed is that the specific access type allows the processing device to perform an operation on the object even while another client has a lock on the object. However, Poublan et al. teach that it is well known that, depending on the particular lock the user has put on the file, reading of the file is still permitted by other processes (where virus-scanning is a "read"-type operation as opposed to a "write" operation). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Bates et al. and Edwards et al. to allow for the processing device to perform an operation, such as virus scanning on the object even while another user has a lock on the object. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Poublan et al. suggest that if a "for input" lock is the type of lock placed on a file by a user, other processes may still access the

file for reading purposes, where this is beneficial so that authorized users may access resources as needed for their duties in col. 63, lines 57-63.

Also not explicitly disclosed is assigning a specific access type to the processing device by the storage server when the storage server verifies the processing device satisfies restriction criteria. The Examiner takes official notice that it is commonly known and widely practiced for the scanning process to be on a device that is assigned a particular access type based on its location in the network, i.e. devices more susceptible to attacks may be given less access than those which are not as vulnerable. It would be obvious to a person skilled in the art to associate the device with a particular access type in order to prevent from various devices gaining unauthorized access to various facilities.

Finally not explicitly disclosed is selecting, at the storage server, the processing device from among a plurality of processing devices that form the cluster, based on classification of the processing device relative to other processing devices in the cluster, wherein the classification is based on performance criteria. However, Bates et al. also suggest distributing the load of generating virus status information (col. 7, line 57- col. 8, line 3). The Examiner takes official notice that it is commonly known and widely practiced in clustered environments to delegate requests to clusters based on their particular load at the time. It would be obvious to a person skilled in the art to assign a particular device within a cluster to a request based on the load on that the device is experiencing at the time the request is received in order to process requests faster within the cluster.

As per claims 92 and 94-95:

Bates et al. and Edwards et al. substantially teach the method/apparatus of claims 90, 85

and 88. Furthermore, Edwards et al. teach wherein the operation includes a plurality of processes (col. 3, lines 60-66). Bates et al. further teach each process being performed at a separate processing device in the cluster (col. 4, lines 48-55).

**References Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. ***US Patent No. 6,801,949 and EP 0903901A2 (filed in Applicant's IDS)*** have been cited because they are relevant due to the manner in which the invention has been claimed ***as recently amended*** (i.e. support the portion relied upon by 'official notice').

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

/Nadia Khoshnoodi/
Examiner, Art Unit 2437
2/1/2009

NK

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437